

PAJ

TI - SECURITY SYSTEM FOR MODEM FOR SUBSCRIBER TELEPHONE LINE

AB - PURPOSE: To prevent an illegal access from a MODEM having no prescribed calculating expression, by generating a random character-string, calculating it by a prescribed calculating expression, collating a result of calculation, and checking the legality of a user.

- CONSTITUTION: In the case of executing a data communication by connecting a terminal side and the center side by a subscriber telephone line, first of all, a terminal side MODEM 1 calls a center side MODEM 2 and a line is connected. After the line is connected, the MODEM 2 generates a random character-string and transmits it to the MODEM 1, and simultaneously, from this random character-string, a result is calculated by a prescribed calculating expression. The MODEM 1 which receives the random character-string executes a calculation by the same calculating expression as the prescribed calculating expression in the MODEM 2 from this random character-string, and transmits a result of calculation to the MODEM 2. The MODEM 2 collates a result of calculation by itself and a result of calculation received from the MODEM 1, and in case when they coincide, an ACK is sent back to the MODEM 1 and a data communication is started, and when they do not coincide, the line is disconnected.

PN - JP63310257 A 19881219

PD - 1988-12-19

ABD - 19890412

ABV - 013150

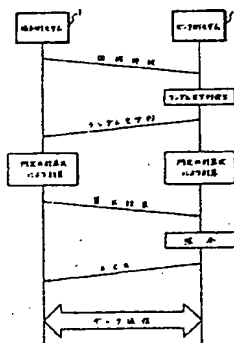
AP - JP19870146675 19870612

GR - E742

PA - NEC CORP

IN - MORITA HIROSHI

I - H04M11/00 ; H04L9/00



<First Page Image>

BEST AVAILABLE COPY

BEST AVAILABLE COPY

⑨ 日本国特許庁 (J.P.)

⑩ 特許出願公開

⑪ 公開特許公報 (A)

昭63-310257

⑫ Int. Cl.⁴

識別記号

庁内整理番号

⑬ 公開 昭和63年(1988)12月19日

H 04 M 11/00
H 04 L 9/00

3 0 3

8020-5K
A-7240-5K

審査請求 未請求 発明の数 1 (全3頁)

⑭ 発明の名称 加入電話回線用モデムのセキュリティ方式

⑮ 特 願 昭62-146675

⑯ 出 願 昭62(1987)6月12日

⑰ 発 明 者 森 田 寛 東京都港区芝5丁目33番1号 日本電気株式会社内
⑱ 出 願 人 日本電気株式会社 東京都港区芝5丁目33番1号
⑲ 代 理 人 弁理士 本 庄 伸 介

明 細 書

1. 発明の名称

加入電話回線用モデムのセキュリティ方式

2. 特許請求の範囲

端末とセンタとを加入電話回線を介して接続するデータ通信システムで利用者の正当性をチェックするセキュリティ方式において、

ランダム文字列を発生する手段と、このランダム文字列を前記端末側モデムへ送信する手段と、前記ランダム文字列を所定の計算式に代入して結果を算出する手段と、前記端末側モデムから送信された算出結果と自らの算出結果とを照合する手段と、前記照合手段により前記2つの算出結果が一致した場合にデータ通信を許可する信号を前記端末側モデムへ送信する手段とを前記センタ側モデムに備え、

前記センタ側モデムから送信された前記ランダム文字列を前記センタ側モデムにおける前記計算

式と同じ計算式に代入して結果を算出する手段と、この算出結果を前記センタ側モデムへ送信する手段とを前記端末側モデムに備えることを特徴とする加入電話回線用モデムのセキュリティ方式。

3. 発明の詳細な説明

(産業上の利用分野)

本発明は、加入電話回線を利用したデータ通信システムにおけるセキュリティ方式に関する。

(従来の技術)

従来、この種のセキュリティ方式は、通信回線を確認した後で、利用者側から単純なパスワードを入力してセンタ側へ送信し、これを照合することにより、利用者の正当性のチェックを行っていた。

(発明が解決しようとする問題点)

上述した従来のセキュリティ方式は、単純なパスワードを照合するだけの簡単なチェックによるものである。従って、特定利用者以外の者が何らかの機会又は方法でパスワードを入手したら、特

定のシステムに対して本来なら利用できない者によるアクセスが生じるという問題点がある。

(問題点を解決するための手段)

上述の問題点を解決するために本発明が提供する加入電話回線用モデムのセキュリティ方式は、端末とセンタとを加入電話回線を介して接続するデータ通信システムで利用者の正当性をチェックするセキュリティ方式であって、ランダム文字列を発生する手段と、このランダム文字列を前記端末側モデムへ送信する手段と、前記ランダム文字列を所定の計算式に代入して結果を算出する手段と、前記端末側モデムから送信された算出結果と、自らの算出結果とを照合する手段と、前記照合手段により前記2つの算出結果が一致した場合にデータ通信を許可する信号を前記端末側モデムへ送信する手段とを前記センタ側モデムに備え、前記センタ側モデムから送信された前記ランダム文字列を前記センタ側モデムにおける前記計算式と同じ計算式に代入して結果を算出する手段と、この算出結果を前記センタ側モデムへ送信する手段と

端末側モデム1から受信した算出結果とを照合し、一致した場合には端末側モデム1へACKを返して、データ通信を開始する。一致しない場合は回線を切断する。

(発明の効果)

以上に説明したように本発明は、ランダム文字列を発生させて、その文字列を所定の計算式で計算することにより算出した結果を照合して、利用者の正当性をチェックする。従って、この所定の計算式を持たないモデムからの不正アクセスを防止できるという効果がある。

また、通信回線に割込まれてセンタ側へ送信する照合値を知られてしまったとしても、所定の計算式に代入する値がランダムに発生する本発明においては、利用することにより照合値が異なるので、何ら支障を生じない。

4. 図面の簡単な説明

第1図は本発明の一実施例の加入電話回線用モデムのセキュリティ方式の動作シーケンス図であ

る。前記端末側モデムに備えることを特徴とする。

(実施例)

以下、本発明の一実施例について図面を参照して説明する。

第1図は本発明の一実施例の加入電話回線用モデムのセキュリティ方式の動作シーケンス図である。

例えば、第1図に示すように、端末側とセンタ側とを加入電話回線で接続してデータ通信を行う場合に、まず、端末側モデム1から端末側モデム1へ発呼して回線を接続する。回線接続後、センタ側モデム2は、ランダム文字列を発生させて端末側モデム1へ送信する。このとき同時に、このランダム文字列から所定の計算式により結果を算出する。センタ側モデム2から送信されたランダム文字列を受信した端末側モデム1は、このランダム文字列からセンタ側モデム2における所定の計算式と同じ計算式により計算し、その算出結果をセンタ側モデム2へ送信する。

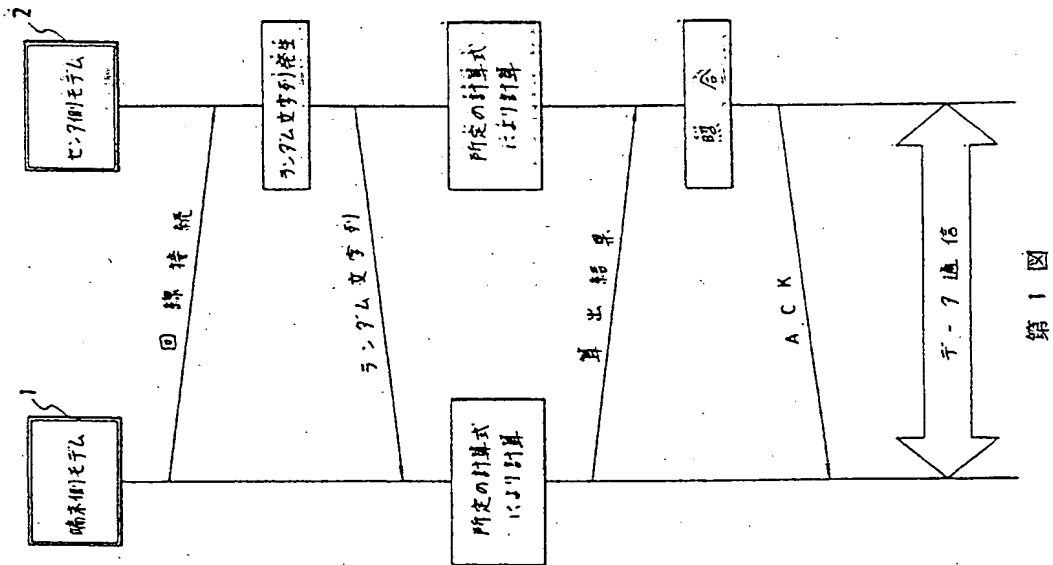
センタ側モデム2では、自ら算出した結果と端

る。

1…端末側モデム、2…センタ側モデム。

代理人 弁理士 本庄伸介

BEST AVAILABLE COPY



第 1 図